

**(12) NACH DEM VERTRÄG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES  
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG**

**(19) Weltorganisation für geistiges Eigentum  
Internationales Büro**



**(43) Internationales Veröffentlichungsdatum  
27. Dezember 2001 (27.12.2001)**

PCT

**(10) Internationale Veröffentlichungsnummer:**  
**WO 01/98899 A2**

(51) Internationale Patentklassifikation<sup>7</sup>: G06F 9/445

**(72) Erfinder; und**

(21) Internationales Aktenzeichen: PCT/CH01/00373

(73) Erfinder/Aufsteller (nur für US): FISCHER, David [CH/CH]; Mühlmattstrasse 61, CH-3007 Bern (CH).

**(22) Internationales Anmeldedatum:**  
15. Juni 2001 (15.06.2001)

(74) Anwalt: FREI PATENTANWALTSBÜRO; Postfach  
768, CH-8029 Zürich (CH).

**(25) Einreichungssprache:** Deutsch

## (26) Veröffentlichungssprache: Deutsch

**(30) Angaben zur Priorität:** 1222/00 20. Juni 2000 (20.06.2000) CH

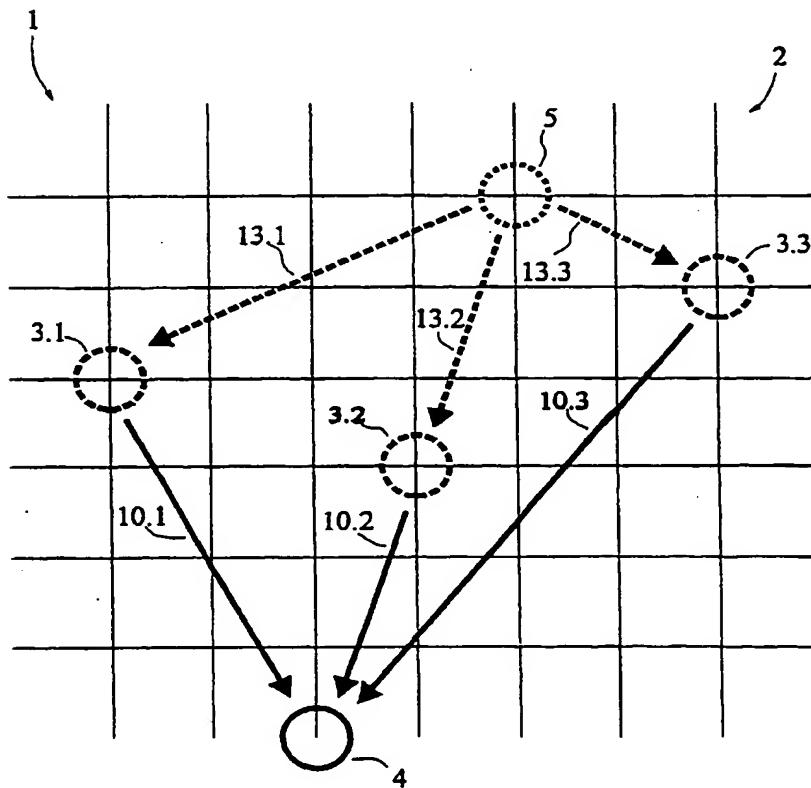
(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): SYSFORMANCE AG [CH/CH]; Badenerstrasse 281, CH-8003 Zürich (CH).

MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

[Fortsetzung auf der nächsten Seite]

**(54) Title: SERVER MONITORING**

**(54) Bezeichnung: SERVERÜBERWACHUNG**



WO 01/98899 A2

**(57) Abstract:** The invention relates to a method for running a plug-in on one or more computers, especially for monitoring purposes. The plug-in is transmitted to at least one computer (11.1, 11.2, 11.3) via a network (2). Afterwards, the plug-in prompts the at least one computer (11.1, 11.2, 11.3) to run this plug-in.

**(57) Zusammenfassung:** Die Erfindung betrifft ein Verfahren um ein Plugin auf einem oder mehreren Computer, insb. zu Überwachungszwecken, zur Ausführung zu bringen. Das Plugin wird über ein Netzwerk (2) an mindestens einen Computer (11.1, 11.2, 11.3) übermittelt. Anschliessend veranlasst das Plugin den mindestens einen Computer (11.1, 11.2, 11.3), dieses zur Ausführung zu bringen.



(84) **Bestimmungsstaaten (regional):** ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Veröffentlicht:**

— ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

## SERVERÜBERWACHUNG

Die vorliegende Erfindung liegt auf dem Gebiet der Netzwerk-, resp. Internettechnologie. Die Aufgabe wird durch die in den Patentansprüchen definierte Erfindung gelöst.

Heute hat sich besonders das Internet als weltweites Kommunikationsmittel etabliert.

5     Die Qualität der angebotenen Dienste spielt daher eine wesentliche Rolle. Firmen die auf dem Internet ihre Dienstleistungen anbieten, haben ein grosses Interesse, dass ihre Server einwandfrei funktionieren und dass unberechtigte Zugriffe frühzeitig erkannt und Massnahmen ergriffen werden können. Eine Überwachung dieser Dienste ist bis heute nicht bekannt. Aus diesem Grund werden viele auf dem Internet angebotene Dienstleistung nicht oder ungenügend in Anspruch genommen. Die Dienste weisen häufig ungenügende Qualität (zu lange Antwortzeiten, usw.) auf, was die potentiellen Benutzer davon abhält. Unberechtigte Zugriffe und Veränderungen werden in der Regel nur sehr schlecht und mit Verzögerung erkannt. Dies führt dazu, dass schädliche Software wie Viren, usw. sich unbemerkt über längere Zeiträume

10    ausbreiten können. Schäden weltweit in Milliardenhöhe sind keine Seltenheit.

15

Es ist Aufgabe der vorliegenden Erfindung ein Verfahren zur Ausführung von Plugins zu zeigen; insbesondere zur Überwachung von Netzwerken, Internetdienstleistungen und Servern.

Die Idee der hier offenbarten Erfindung basiert u.a. darauf, eine Proxy-Server Unterstützung des Internet HTTP-Protokolls zum Zweck der automatischen Aufzeichnung und der späteren automatischen Wiederabspielung eines Datenverkehrs von einem oder mehreren HTTP-Clients (z.B. Web-Browsern), die mit einem HTTP-Server oder HTTP-Proxy-Server kommunizieren, zu verwenden. Vorzugsweise referentiell aufgezeichnete Daten werden dabei in einer Form gespeichert, die es erlaubt den vollständigen Datenverkehr der vom Client und vom Server generiert wird (Requests), zu einem späteren, bestimmbaren Zeitpunkt automatisch und beliebig oft, insb. von verschiedenen geographischen Orten aus und unter Einhaltung von definierten Kriterien zu wiederholen, zu überwachen und auszuwerten. Der Vorgang erfolgt in der Regel ohne Zutun des ursprünglichen, generierenden Clients. Bei der Aufzeichnung eines Datenverkehrs werden üblicher Weise auch die Antwort-Daten des Servers (Responses) ganz oder teilweise aufgezeichnet. Dadurch ist es erstmals möglich, dass bei einer späteren Anwendung der aufgezeichneten Client-Requests kontrolliert werden kann, ob der Server analoge, gleichbleibende Daten liefert, oder ob er von einer definierten Norm abweicht. Dies spielt zur periodischen Überwachung von unberechtigten Zugriffen eine relevante Rolle.

Im Zusammenhang mit der Überwachung z.B. von Viren wird bei Bedarf anstelle einer meist erfolglosen Suche nach schädlichen Programmen, die Information periodisch mit gesicherten und vertrauenswürdigen Referenzdaten (von einem oder mehreren entfernten Standpunkten aus) verglichen. Eine entsprechender Vergleich liefert aussagekräftige Daten mit minimalem Aufwand. So ist es z.B. möglich, dass eine Firma entsprechende Dienste anbietet indem Sie Referenzdaten von einzelnen Servern periodisch mit deren momentanen Verhalten, z.B. zwecks Qualitätssicherung, vergleicht und überwacht. Bei Bedarf werden die Antwortzeiten des Servers aufgezeichnet. Die Überwachung erfolgt vorteilhafter Weise von verschiedenen geographischen Orten aus, derart, dass eine Überwachung über mehrere Kanäle erfolgt. Damit ist es zudem möglich die Performance und Abweichungen derselben von definierba-

ren Grenzwerten (insb. über unterschiedliche Wege) zu vergleichen und auszuwerten. Entsprechend Alarmmeldungen werden falls erforderlich abgesetzt.

Der Inhalt des Datenverkehrs über ein gewähltes Protokoll (bspw. HTTP) spielt beim hier beschriebenen Verfahren eine eher untergeordnete Rolle, d.h. es können sämtliche Inhalte aufgezeichnet und wieder abgespielt werden, auch wenn diese z.B. Inhalte von höher liegenden Protokollen, wie z.B. JavaScript oder SSL, betreffen. Weitere Anwendungsbeispiele des hier beschriebenen Verfahrens sind, z.B. das Aufzeichnen von interaktiven Webbrowser Surfsessions. Dabei ist es vorteilhaft eine Referenz-Session aus einer oder mehreren Sessions zu generieren. Eine Auswertung und ein späteres Anwenden dieser Surf-Sessions z.B. in Form von Last-Test-Routinen dient der referentiellen Überwachung und der Kontrolle von unberechtigten Zugriffen, sowie der Performancemessung. Insbesondere wird auch die Verfügbarkeit des Servers überwacht, um Hardwaredefekte oder Abstürze zu überwachen. Ein Vergleich der referenzierten (aufgezeichneten) Server-Antwortdaten mit dem bei einer Anwendung derselben auf einen Server, insb. über mehrere Kanäle oder Pfade, generierten Datenverkehr wird bevorzugt als Mechanismus zur Erkennung von Modifikationen des Dateninhalts des Servers sowie zur ortsabhängigen Performancemessung eingesetzt. Illegale Zugriffe und Veränderungen werden damit zuverlässig und schnell erkannt.

Normalerweise sind die z.B. im heute weit verbreiteten HTTP-Protokoll vorgesehnen Einsatzzwecke von Proxy-Servern u.a. die folgenden: Zwischenspeichern von Daten, zum Zweck der Verkürzung der Antwortzeiten; Protokollierung und Auswertung des Datenverkehrs zwischen Client und Server, im Hinblick auf die Kontrolle des Surf-Verhaltens individueller natürlicher Personen (Beobachtung und Kontrolle der Person, Unterdrückung unerwünschter Websites etc.); Unterbindung der direkten Verbindung einzelner Computer von Endbenutzern mit dem Internet aus Sicherheitsgründen. Die hier offenbarete Erfindung basiert in entfernter Weise auf der

Funktionalität eines Proxy-Servers auf. Im Unterschied hierzu wird die eigentliche Hauptfunktion eines herkömmlichen Proxy-Servers dabei nicht oder nur in neben-sächlicher Weise verwendet. Die hier offenbare Erfindung weist zu einem herkömmlichen Proxy-Server u.a. die folgenden Unterschiede auf:

- 5
  - Damit alle Dateninhalte zwischen Client und Server werden (zeitlich) kompakt aufgezeichnet werden können, werden bei der Erfindung sämtliche Cache- Mechanismen (sowohl des normalen HTTP-Protokolls sowie auch des HTTP-Proxy- Protokolls, insb. der direkt dargestellten und der vom Client ausgeführten Referenzen) ausser Acht gelassen (bei Bedarf kann eine Verwendung vorgesehen werden) oder unterdrückt. Die Erfindung erfordert daher in der Regel keinen eigenen Cache.
- 10
  - Insbesondere werden gezielt alle Informationen des Clients an den Server und des Servers an den Client über Cache-Möglichkeiten unterdrückt, um zu erreichen, dass alle relevanten Daten übermittelt werden.
- 15
  - Die Erfindung weist Mittel zur Aufzeichnung auf. Mit eigens dafür vorgesehenen Schnittstellen werden diese Mittel gesteuert ("Start Record"). In diesem Zustand werden alle Requests/Responses in einer definierten Datenstruktur gespeichert so, dass der Verlauf derselben zu einem späteren Zeitpunkt mit entsprechenden Mittel (beispielsweise einer entsprechend programmierten Maschine) nachvollzogen werden können. Die z.B. referentiell aufgezeichneten Daten werden mit Vorteil in einer entsprechenden Bibliothek angelegt.
- 20
  - Aus den aufgezeichneten Daten werden bei Bedarf automatisch oder manuell erfindungsgemäss Plugins erzeugt (vgl. hierzu weiter unten), die über erfindungsgemä-

Aus den aufgezeichneten Daten werden bei Bedarf automatisch oder manuell erfindungsgemäss Plugins erzeugt (vgl. hierzu weiter unten), die über erfindungsgemä-

sse Mittel, z.B. Sonden (vgl. hierzu weiter unten), ausführbar sind, derart dass insb. von unterschiedlichen Orten aus der selbe Test gleichzeitig durchführbar ist. Damit ist es möglich einen Server mit verschiedenen oder mehrere Server mit speziellen Referenzdaten zu überwachen. Die Erfindung lässt sich auf nur einen Client gezielt 5 oder aber auf alle Clients anwenden. Bei Clients mit einer separaten Aufzeichnung wird vorteilhafter Weise vom Client eine HTTP-Authentication verlangt. Diese kann bei jedem Request eines Clients danach dazu benutzt werden, um die Aufzeichnungsdaten der einzelnen Clients einzeln zu führen.

Es versteht sich von selber, dass die Erfindung falls erforderlich auch HTTP zu 10 HTTPS (SSL) Konvertierungen bzw. höher liegende Protokolle unterstützen kann. Beispielsweise können, zum Aufzeichnen von HTTPS-Abfragen, vom Client unverschlüsselte Anfragen an den Server gemacht werden. Diese unverschlüsselten Anfragen werden dann erst durch die Erfindung verschlüsselt und an den Server weitergeleitet. Die Antwort wird wiederum durch die Erfindung entschlüsselt und an den Client 15 zurück geleitet. Dabei ist es besonders vorteilhaft, dass das SSL-Protokoll durch die Erfindung entschlüsselt wird und nicht erst durch den Client. Dadurch ist es möglich, den Datenaustausch zwischen Client und Server auch bei einer Verschlüsselung aufzuzeichnen. Höherliegende Protokolle werden zum Zweck der Aufzeichnung/Überwachung gezielt aufgebrochen, indem Anstelle eines vorgesehenen Tunnel- 20 ling-Verfahrens eine Client-Server-Client-Server Verfahren vorgesehen wird.

Aus dem Stand der Technik sind Plugins bekannt. Plugins sind typischerweise universell einsetzbare Programme, die darauf spezialisiert sind, irgendeine Funktion auszuführen. Um ein Plugin zu aktivieren ist eine entsprechende Plugin-Schnittstelle erforderlich. Bei Java-Programmen beispielsweise erfolgt dies über ein entsprechendes Interface. In der Regel ist es so, dass ein Plugin aufgrund einer Anfrage bzw. 25 eines Bedarfs eines Programms geladen wird (z.B. von einem Web-Browser). So- wohl bei CORBA als auch bei RMI (Java Remote Method Invocation) werden aber,

im Unterschied zur hier offenbarten Erfindung, nur Daten, bzw. Variablen ausgetauscht, es wird jedoch kein Programmcode übermittelt. Bei den erfindungsgemässen Plugins wird im Unterschied zum Stand der Technik typischerweise der Programm-Code übertragen. Bei konventionellen Plugins geht zudem der Anreiz zum Laden eines Plugins immer von dem Ort aus, an dem das Plugin auch ausgeführt wird (von innen). Bei erfindungsgemässen Plugins kommt dieser Anreiz jedoch von einem anderen Ort, also typischerweise von aussen.

Die erfindungsgemässen Plugins funktionieren vorteilhafter Weise wie folgt: An einem ersten Ort (Ausgangsort) wird zu einem bestimmten Zeitpunkt veranlasst, dass ein Plugin an einem zweiten Ort (Zielort) mittels einem geeigneten Mittel ausgeführt werden soll. Das Plugin wird darauf an den zweiten Ort (Zielort) mit einer Aufforderung zur Ausführung übertragen. Das Resultat besteht also darin, dass am zweiten Ort (Zielort) ein Plugin ausgeführt wird welches z.B. ein Resultat an den ersten Ort (Ausgangsort) zurückgemeldet. Einzige Anforderung am zweiten Ort (Zielort) ist, dass erfindungsgemäss Plugins empfangbar, resp. ausführbar (= „anspringen“) sind. Es ist nicht erforderlich, dass der Zielort über den Inhalt des erfindungsgemässen Plugins etwas weiss. Aus Sicherheits-Gründen kann aber ein erfindungsgemässes Plugin am Zielort gewissen, von aussen sicht- oder unsichtbaren Beschränkungen unterliegen. So kann z.B. festgelegt werden, dass ein erfindungsgemässes Plugin eine bestimmte Ausführungszeit nicht überschreiten darf, etc. Wird eine Verletzung einer entsprechenden Beschränkungen registriert, so werden entsprechende Massnahmen ergriffen, indem beispielsweise die Ausführung abgebrochen wird (d.h. das Plugin wird „getötet“). Bei einer Realisierung von erfindungsgemässen Plugins, bspw. mittels der Programmiersprache "Java", wird mittels eines speziellen Class-Loaders am Zielort „auf Befehl“ bestimmte Plugins als "Class" geladen. Anschliessend wird davon eine "Instanz" erzeugt, welche dann z.B. über ein Plugin-Interface aufgerufen wird.

Die erfindungsgemässen Plugins werden in der Regel automatisch mittels einer erfindungsgemässen Anordnung erzeugt. Dabei werden in der Regel interaktiv generierte Daten z.B. von Surfsessions verwendet. Bei den generierten Plugins handelt es sich typischerweise um ausführbaren Programmcode. Ein wesentlicher Unterschied 5 zum Stand der Technik besteht u.a. darin, dass die erfindungsgemässen Plugins in der Regel automatisch generiert werden. Ein erfindungsgemässer Recorder, der u.a. zur Erzeugung von Plugins dient, hat vorteilhafter Weise ein Web-Interface in der Art, dass auch ein technisch nicht versierter Benutzer z.B. eine Surfsession aufzeichnen kann, um diese danach in die zentrale Datenbank von Testanordnungen einzubringen, resp. diese als Plugin zu erstellen. Diese Surfsession steht ab dann zur Verfügung um Tests jeglicher Art in periodischen oder willkürlichen Zeitintervallen z.B. 10 durch Sonden auszuführen. Diese bewusste End-User-Funktionalität, die derart konzipiert ist, dass sie ohne technisches Wissen bedienbar ist, bietet zusätzliche Vorteile.

15 Die Erfindung wird anhand der folgenden Figur näher erläutert. Diese zeigt schematisch ein Netzwerk mit Sonden und einem zentralen Dienst.

Figur 1 zeigt eine vorteilhafte Ausführungsform der Erfindung. Ein erfindungsgemässes Überwachungssystem 1 überwacht über ein Netzwerk (Inter-/Intranet) 2, bei Bedarf von verschiedenen Punkten 3.1, 3.2, 3.3 aus, beliebige Services von einem Host 4 mit Hilfe eines zentralen Dienstes, der bevorzugt mittels einem zentralen System 20 5 betrieben wird. Test-Konfigurationen, Test-Programme, beispielsweise in Form von erfindungsgemässen Plugins, und auch Test-Resultate werden bevorzugt in einer Datenbank gespeichert, die sich hier im Bereich des zentralen Systems 5 befindet. Auf dem zentralen System 5 läuft ein Programm, welches vorbestimmte oder zufällige Testkonfigurationen periodisch und oder aperiodisch, z.B. zu Überwachungszwecken, oder einmalig über viele Instanzen/Kanäle 10.1, 10.2, 10.3 parallel, 25 z.B. als Lasttest, zur Ausführung bringt. Das zentrale System 5 führt jedoch diese Tests in der Regel nicht selbst aus, sondern übermittelt Test-Programme und Test-

Konfigurationen an eigens dafür vorgesehene Mittel, hier Sonden (Computer) 11.1, 11.2, 11.3. Diese befinden sich vorzugsweise örtlich getrennt in einem Netzwerk 2, z.B. bei Providern, in einem Rechenzentrum, usw. In der Regel geschieht die Übermittlung gleichzeitig an mehrere Sonden (schematisch durch Pfeile 13.1, 13.2, 13.3 dargestellt). Diese führen einen oder mehrere Tests aus und übermitteln ortsabhängige Resultate an ein zentrales System. Hierbei kann es sich um dasselbe oder ein anderes zentrales System handeln. Das zentrale System 5 (oder bei Bedarf auch eine oder mehrere Sonden 11.1, 11.2, 11.3) analysiert und speichert die Resultate und veranlasst gegebenenfalls weitere Reaktionen (z.B. Alarm auslösen). Beim erfindungsgemässen Verfahren wird ein Plugin zur Ausführung gebracht, indem es über ein Netzwerk (2) an mindestens einen Computer (11.1, 11.2, 11.3) übermittelt wird. Das Plugin veranlasst anschliessend den mindestens einen Computer (11.1, 11.2, 11.3), das Plugin zur Ausführung zu bringen.

15 Durch die erfindungsgemäss Anordnung von einem oder mehreren zentralen Systemen 5 und einer oder mehreren Sonden 11.1, 11.2, 11.3 kann an unterschiedlich (geografischen) Orten im Intranet oder Internet getestet werden, ob z.B. ein zu überwachendes Zielsystem/Server 4 erreichbar und/oder funktionsfähig ist oder ob es gewisse Eigenschaften hat oder ob eine lokale Eigenschaft bei einer Sonde vorhanden und ggf. funktionsfähig ist. Beispielsweise wird ein Web-Server von mehreren Sonden aus überprüft. Dabei wird insbesondere getestet, ob der Webserver von den einzelnen Sonden her, also von unterschiedlichen geografischen Punkten aus, erreichbar ist. Ist der Webserver erreichbar, so wird z.B. auch der „Inhalt“ des Web-Servers getestet werden (Verhalten auf HTTP-Requests). Ebenfalls wird bei Bedarf ein Lasttest durchgeführt werden. Wesentlich ist, dass der Server nicht nur von einem Punkt aus, sondern von vielen überwacht wird.

20

25

Die beschriebene erfindungsgemäße Systemarchitektur, bei der von mehreren, örtlich getrennten Punkten aus operiert wird, ergänzt mit erfindungsgemäßen Plugins, die auf Sonden ausgeführt werden, ergibt ein universelles Testsystem, dass fast jeden erdenklichen Test in einem Intranet bzw. im Internet ausführen kann, ohne dass für 5 unterschiedliche Tests die ganze System-Architektur wieder neu programmiert oder ergänzt werden muss. Es genügt in der Regel, dass ein neues erfindungsgemässes Plugin typischerweise automatisch mittels einem erfindungsgemässen Recorder erzeugt wird und in einer Datenbank eines des zentralen Systems gespeichert wird.

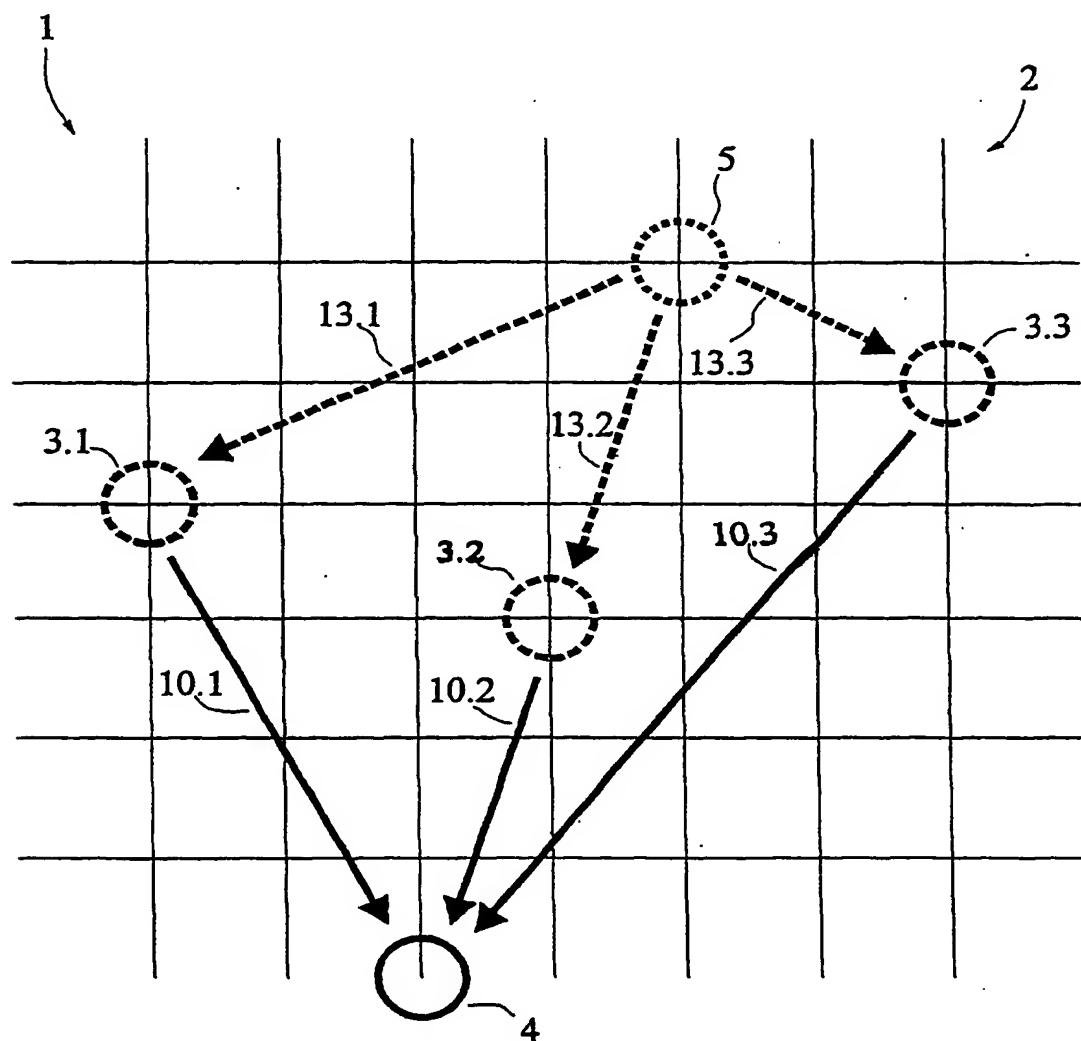
## PATENTANSPRÜCHE

1. Verfahren um ein Plugin zur Ausführung zu bringen, dadurch gekennzeichnet, dass das Plugin über ein Netzwerk (2) an mindestens einen Computer (11.1, 11.2, 11.3) übermittelt wird und dass dieses Plugin anschliessend den mindestens einen Computer (11.1, 11.2, 11.3) veranlasst, das Plugin zur Ausführung zu bringen.  
5
2. Verfahren gemäss Patentanspruch 1, dadurch gekennzeichnet, dass das Plugin aus einer Datenbank von vielen Plugins entnommen wird.
3. Verfahren gemäss einem der vorangehenden Patentansprüche, dadurch gekennzeichnet, dass das Plugin automatisch mittels einer interaktiven Surfsession generiert wird.  
10
4. Verfahren gemäss einem der vorangehenden Patentansprüche, dadurch gekennzeichnet, dass das Plugin an mehrere, örtlich getrennte Computer (11.1, 11.2, 11.3) übermittelt wird und dass das Plugin diese Computer (11.1, 11.2, 11.3) veranlasst das Plugin gleichzeitig oder ungleichzeitig zur Ausführung zu bringen.  
15
5. Verfahren gemäss einem der vorangehenden Patentansprüche, dadurch gekennzeichnet, dass das auf dem mindestens einen Computer (11.1, 11.2, 11.3) zur Ausführung gebrachte Plugin den mindestens einen Computer (11.1, 11.2,

11.3) veranlasst Daten an einen weiteren über ein Netzwerk (2) verbundenen Computer (4) zu Überwachungszwecken zu übermitteln.

6. Verfahren gemäss Patentanspruch 5, dadurch gekennzeichnet, dass der weitere über ein Netzwerk (2) verbundene Computer (4) veranlasst wird Daten an einen Computer (11.1, 11.2, 11.3) zu übermitteln.  
5
7. Computerprogramm beinhaltend Computerprogrammcode, dadurch gekennzeichnet, dass es geeignet ist mindestens einen Computer (11.1, 11.2, 11.3) dazu zu veranlassen die Schritte des Verfahrens gemäss einem der Patentansprüche 1 bis 6 auszuführen.
- 10 8. Computerlesbares Medium beinhaltend Computerprogrammcode, dadurch gekennzeichnet, dass es geeignet ist mindestens einen Computer (11.1, 11.2, 11.3) dazu zu veranlassen die Schritte des Verfahrens gemäss einem der Patentansprüche 1 bis 6 auszuführen.

1/1

**Fig. 1**